

UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF WASHINGTON
AT TACOMA

ABHI SHETH, individually and on behalf of all
others similarly situated,

Plaintiff,

v.

WASHINGTON STATE UNIVERSITY,

Defendant.

CLASS ACTION COMPLAINT FOR:

1. Negligence;
2. Violation of the Washington Data Disclosure Law, RCW § 19.255.010-020; and
3. Violation of the Washington Consumer Protection Act, RCW § 19.86, *et seq.*

JURY TRIAL DEMANDED

Plaintiff Abhi Sheth (“Plaintiff”), by and through his counsel, brings this Class Action Complaint against Defendant Washington State University (“Defendant”) on behalf of himself and all others similarly situated, and alleges, upon personal knowledge as to his own actions and his counsel’s investigations, and upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. This class action arises from a hard drive Defendant had stolen from its storage unit in or around April 2017 (the “Data Breach”). The hard drive contained personal information of approximately one million people, including personal identifying information

1 (“PII”) such as names, Social Security numbers, and personal health information (“PHI”), some
2 of which may not have been encrypted.

3 2. The hard drive contained PII and PHI from individuals, like Plaintiff, who were
4 being tracked by Defendant for research purposes over the course of 15 years: (1) tracking high
5 school students after graduation to see if they’re going to college or getting jobs; and (2)
6 tracking clients of state job-training programs to see if they were able to find jobs.

7 3. Despite learning of the Data Breach on or about April 21, 2017, Defendant did
8 not publicly announce or notify the affected individuals until June 9, 2017, seven weeks later.
9 Defendant’s notification and the information it has disclosed to date has been vague and
10 incomplete, and it has offered merely one-year of complimentary credit monitoring and identity
11 theft protection.

12 II. PARTIES

13 4. Plaintiff is a resident of Seattle, Washington. Plaintiff was unemployed for
14 approximately six months in 2009 and approximately four months in 2013 and participated in a
15 state job-training program. On or about April 29, 2017, Plaintiff suffered a fraudulent online
16 charge on one of his lines of credit for \$196.58. Plaintiff had to file a fraud claim with the
17 vendor. In June 2017, Plaintiff received a letter from Defendant in the mail dated June 9, 2017,
18 notifying him that his information was compromised in the Data Breach.

19 5. Defendant is a state public research university, with its main office located
20 within this District at 1155 College Avenue, Pullman, Washington 99164-2114, as well as other
21 campus locations throughout the District.

22 III. JURISDICTION AND VENUE

23 6. This Court has original jurisdiction over this action under the Class Action
24 Fairness Act (CAFA), 28 U.S.C. § 1332(d), because this is a class action in which (i) the
25 proposed class consists of more than 100 members; (ii) at least some members of the proposed
26
27

1 class are citizens of a state different from any defendant; and (iii) the matter in controversy
2 exceeds \$5,000,000, exclusive of interest and costs.

3 7. This Court has personal jurisdiction over Defendant because Defendant is
4 authorized to, and does, business in the State of Washington, providing conducting research on
5 to citizens of this State, including Plaintiff.

6 8. Venue is proper in this District pursuant to 28 U.S.C. § 1391(a) because
7 Defendant resides in this District and a substantial part of the events that give rise to the claims
8 herein occurred in this District.

9 **IV. FACTUAL BACKGROUND**

10 9. In or around April 2017, the Data Breach occurred when an 85-pound safe was
11 stolen from a storage locker at Defendant's facility in Olympia, Washington. Inside the safe
12 was a hard drive containing the names, Social Security numbers, and PHI of approximately one
13 million individuals. Some of the data on the hard drive was not encrypted.

14 10. The Olympia facility is used as off-site storage by Defendant's Social &
15 Economic Sciences Research Center ("SESRC"). The SESRC is a research arm of the
16 university that contracts with state agencies to evaluate data those agencies collect.

17 11. The hard drive was a backup storing data of one million individuals collected
18 by: (1) school districts tracking students after graduation to see if they go to college or get jobs;
19 and (2) state job-training programs tracking clients to see if they were able to get jobs. The
20 data had been collected over a 15-year period, from 1998 to 2013, for long-term studies by
21 Defendant.

22 12. As a result of Defendant's deficient security, Defendant reportedly is now
23 conducting a "top to bottom" review of its information and technology practices and policies,
24 including where and how it stores backup hard drives and how it handles PII. On information
25 and belief, Defendant failed to properly segregate PHI from other PII.

1 13. PII, and especially PHI, is highly valuable on underground criminal exchanges
2 where stolen data is sold because the information can be used to engage in insurance fraud, and
3 because the information involved can be used to engage in a variety of other crimes, including
4 financial identity theft, for instance by using Social Security numbers to open new accounts in a
5 victim's name.

6 14. Defendant did not disclose the Data Breach until June 9, 2017, despite having
7 known about it at least seven weeks earlier, since April 21, 2017, according to Defendant's own
8 account of events.

9 15. Defendant has not yet fully and accurately informed the affected individuals
10 regarding the scope of the Data Breach or the risks of identity theft. It is not clear how many
11 people it has notified to date, and its notification letters are vague and do not contain sufficient
12 information regarding the Data Breach.

13 16. It is critical that companies affected by data breaches provide timely, accurate,
14 and complete information to those whose information has been compromised so they can take
15 necessary precautions to protect themselves and their families from further harm. Washington
16 state law requires Defendant to provide notice in the most expedient time possible. *See* RCW
17 § 19.255.010.

18 17. As a result of the Data Breach, Plaintiff and Class members will have to take a
19 variety of steps to monitor for and safeguard against identity theft and are at a much greater risk
20 of suffering such identity theft, which may well include fraudulent medical care in the victims'
21 names, charges for such medical care, and/or adulteration of the victims' true medical records
22 in possibly dangerous ways. In addition, these victims of the Data Breach are at a heightened
23 risk of potentially devastating financial identity theft. As the Bureau of Justice Statistics
24 reports, identity theft causes its victims out-of-pocket monetary losses and costs the nation's
25 economy billions of dollars every year. *See* U.S. Dept. of Justice, Bureau of Justice Statistics,
26
27

1 *Victims of Identity Theft, 2012* (Dec. 2013), available at

2 <<http://www.bjs.gov/content/pub/pdf/vit12.pdf>> (last visited Mar. 30, 2015).

3 18. Loss of Social Security numbers, such as those disclosed through the Data
4 Breach that Defendant failed to prevent, can be especially devastating, as thieves can use such
5 information, in combination with the other PII stolen, to open new accounts in victims' names
6 without their knowledge, and even to obtain fraudulent encumbrances on such victims'
7 property.

8 19. Consequently, Plaintiff has already suffered a fraudulent online charge on one of
9 his existing lines of credit. The fraud occurred on or about April 29, 2017, only about one
10 week after Defendant purportedly learned of the Data Breach. Plaintiff is taking steps to
11 mitigate this fraud and protect against future fraudulent activity as a result of the Data Breach.
12 Plaintiff will have to expend time and money to protect himself that he otherwise would not
13 have spent if the Data Breach had not occurred.

14 20. Defendant breached its duty (a) to protect and safeguard these individuals' PII
15 and PHI, and (b) to notify those affected in a timely and complete manner. Plaintiff brings this
16 action on behalf of himself and similarly situated insureds whose PII and PHI was
17 compromised in the Data Breach, for compensation for the injuries they have suffered and for
18 injunctive relief to ensure that Defendant takes proper security precautions in the future and
19 gives prompt and full information to all affected people concerning their exposure in the Data
20 Breach.

21 **V. CLASS ACTION ALLEGATIONS**

22 21. Plaintiff brings this action on behalf of a nationwide class preliminarily defined
23 as:

24 All individuals residing in the United States whose personal and/or medical
25 information was compromised in the data breach disclosed by Washington State
26 University on or about June 9, 2017.
27

(The “Nationwide Class.”) Excluded from the Nationwide Class are Defendant; any agent, affiliate, parent, or subsidiary of Defendant; any entity in which Defendant has a controlling interest; any officer or director of Defendant; any successor or assign of Defendant; and any Judge to whom this case is assigned as well as his or her staff and immediate family.

22. Plaintiff also brings this action on behalf of a Washington State Class, preliminarily defined as:

All individuals residing in the State of Washington whose personal and/or medical information was compromised in the data breach disclosed by Washington State University on or about June 9, 2017.

(The “Washington Class.”) Excluded from the Washington Class are Defendant; any agent, affiliate, parent, or subsidiary of Defendant; any entity in which Defendant has a controlling interest; any officer or director of Defendant; any successor or assign of Defendant; and any Judge to whom this case is assigned as well as his or her staff and immediate family.

23. These classes are collectively referred to herein as the “Class.” Plaintiff reserves the right to amend these class definitions.

24. Plaintiff satisfies the numerosity, commonality, typicality, and adequacy prerequisites for suing as a representative party under Rule 23.

25. **Numerosity.** The proposed Class reportedly consists of approximately one million members—far too many to join in a single action, and although the Washington Class may be slightly smaller, on information and belief the Washington Class consists of thousands of members, at a minimum, and also satisfies the numerosity requirement.

26. **Ascertainability.** Class members are readily identifiable from information in Defendant’s possession, custody, or control.

27. **Typicality.** Plaintiff’s claims are typical of Class members’ claims as each arises from the same Data Breach, the same alleged negligence of and/or statutory violations by

1 Defendant, and the same unreasonable manner of notifying Defendant's insureds regarding the
2 Data Breach.

3 28. **Adequacy.** Plaintiff will fairly and adequately protect the interests of the
4 proposed Class. His interests do not conflict with Class members' interests and he has retained
5 counsel experienced in complex class action litigation and medical data privacy to vigorously
6 prosecute this action on behalf of the Class.

7 29. **Commonality.** Plaintiff's and Class members' claims raise predominantly
8 common factual and legal questions that can be answered for all Class members through a
9 single class-wide proceeding. For example, to resolve any Class member's claims, it will be
10 necessary to answer the following questions. The answer to each of these questions will
11 necessarily be the same for each class member.

- 12 A. Whether Defendant unlawfully used, maintained, lost or disclosed Class
13 members' personal, financial, and/or other information;
- 14 B. Whether Defendant unreasonably delayed in notifying affected
15 individuals of the Data Breach and whether the belated notice was
16 adequate;
- 17 C. Whether Defendant failed to implement and maintain reasonable security
18 procedures and practices appropriate to the nature and scope of the
19 information compromised in the Data Breach;
- 20 D. Whether Defendant's conduct was negligent;
- 21 E. Whether Defendant's conduct in connection with the Data Breach and
22 notification thereof violated Washington State law;
- 23 F. Whether Plaintiffs and the Class are entitled to damages, civil penalties,
24 punitive damages, and/or injunctive relief.

25 30. In addition to satisfying the prerequisites of Rule 23(a), Plaintiff satisfies the
26 requirements for maintaining a class action under Rule 23(b). Common questions of law and
27

fact predominate over any questions affecting only individual members and a class action is superior to individual litigation. The damages available to individual plaintiffs are insufficient to make litigation addressing Defendant's medical privacy practices economically feasible in the absence of the class action procedure.

31. In the alternative, class certification is appropriate because Defendant has acted or refused to act on grounds generally applicable to the class, thereby making final injunctive relief appropriate with respect to the members of the class as a whole.

VI. FIRST CAUSE OF ACTION

Negligence

(On Behalf of Plaintiff and All Classes)

32. Plaintiff incorporates by reference all foregoing factual allegations.

33. Defendant collected and stored PII and PHI from Plaintiff and Class members to conduct long-term studies for contractual obligations with other state-run educational entities.

34. Defendant assumed a duty of care to use reasonable means to secure and safeguard this PII and PHI, to prevent disclosure of the information, to guard the information from theft, and to detect any attempted or actual breach of its IT systems.

35. Defendant breached its duty of care by failing to secure and safeguard the PII and PHI of Plaintiff and Class members. Defendant negligently stored the data knowing it was vulnerable to a security breach. Defendant negligently stored PII and PHI in a partially unencrypted form on a highly vulnerable device.

36. Defendant continues to breach this duty of care by failing to share crucial, complete information with Plaintiff and Class members in a timely manner.

37. Plaintiff and Class members have suffered harm as a result of Defendant's negligence. These victims' loss of control over the PII and PHI exposed subjects each of them to a greatly enhanced risk of identity theft, medical identity theft, credit and bank fraud, Social Security fraud, tax fraud, and myriad other types of fraud and theft. Plaintiff and Class

1 members suffered and continue to suffer further harm by virtue of Defendant's failure to give
2 timely and complete notice to them concerning the Data Breach and the risks they face.

3 **VII. SECOND CAUSE OF ACTION**

4 **Violation of the Washington Data Disclosure Law, RCW § 19.255.010-020**

5 **(On Behalf of Plaintiff and All Classes)**

6 38. Plaintiff incorporates by reference all foregoing factual allegations.

7 39. Under RCW § 19.255.010, Defendant is required to disclose "any breach of the
8 security of the data immediately following discovery" of a data breach, "in the most expedient
9 time possible and without unreasonable delay."

10 40. Under RCW § 19.255.020, Defendant is required to exercise "reasonable care to
11 guard against unauthorized access to" the PII and PHI disclosed in the Data Breach.

12 41. By waiting seven weeks after discovering the Data Breach, Defendant failed to
13 disclose the Data Breach in the most expedient time possible, and failed to exercise reasonable
14 care to prevent the Data Breach.

15 42. Plaintiff seeks damages as permitted by law, as well as injunctive relief. As of
16 this filing, Defendant has not provided notice to victims of the Data Breach consistent the
17 requirements of Washington law, and it should be compelled to do so without delay.

18 **VIII. THIRD CAUSE OF ACTION**

19 **Violation of the Washington Consumer Protection Act, RCW § 19.86, *et seq.***

20 **(On Behalf of Plaintiff and All Classes)**

21 43. Plaintiff incorporates by reference all foregoing factual allegations.

22 44. Defendant is a "person" within the meaning of the Washington Consumer
23 Protection Act, RCW § 19.86.010(1), and conducts "trade" and "commerce" within the
24 meaning RCW § 19.86.010(2).

25 45. Plaintiff and other members of the classes are "persons" within the meaning of
26 RCW § 19.86.010(1).
27

1 46. Defendant's failure to safeguard the PII and PHI disclosed in the Data Breach
2 constitutes an unfair act that offends public policy, including as set forth in the foregoing state
3 laws.

4 47. Defendant's failure to promptly and fully notify Plaintiff and Class members
5 regarding the Data Breach is unfair and/or deceptive because these acts or practices offend
6 public policy and omit to disclose material information timely to Plaintiff and Class members,
7 including as set forth in the foregoing state laws.

8 48. Defendant's failure to safeguard the PII and PHI disclosed in the Data Breach,
9 and its failure to provide timely and complete notice of that Data Breach to the victims, causes
10 substantial injury to Plaintiff and Class members, is not outweighed by any countervailing
11 benefits to consumers or competitors, and is not reasonably avoidable by consumers.

12 49. Defendant's failure to safeguard the PII and PHI disclosed in the Data Breach,
13 and its failure to provide timely and complete notice of that Data Breach to the victims, is
14 unfair because these acts and practices are immoral, unethical, oppressive, and/or unscrupulous.

15 50. Defendant's unfair acts or practices occurred in its trade or business and have
16 and are capable of injuring a substantial portion of the public. Defendant's general course of
17 conduct as alleged herein is injurious to the public interest, and the acts complained of herein
18 are ongoing and/or have a substantial likelihood of being repeated.

19 51. As a direct and proximate result of Defendant's unfair acts or practices, Plaintiff
20 and Class members suffered injury in fact.

21 52. Plaintiff and Class members are entitled to an order enjoining the conduct
22 complained of herein and ordering Defendant to take remedial measures to prevent similar data
23 breaches; actual damages; treble damages pursuant to RCW § 19.86.090; costs of suit,
24 including reasonable attorneys' fees; and such further relief as the Court may deem proper.
25
26
27

IX. PRAYER FOR RELIEF

WHEREFORE, Plaintiff makes the following prayer for relief, on behalf of himself and the proposed Class:

- A. An order certifying the proposed Class pursuant to Federal Rule of Civil Procedure 23 and appointing Plaintiff and his counsel to represent the Class;
- B. An order awarding Plaintiff and Class members monetary relief, including actual and statutory damages;
- C. Equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class members' PII and PHI, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiff and Class members;
- D. Equitable relief compelling Defendant to utilize appropriate methods and policies with respect to its data collection, storage, and safety practices and to disclose with specificity to Class members the type of data compromised in the Data Breach, and other information required under the laws cited herein;
- E. Equitable relief requiring restitution and disgorgement of the revenues wrongfully retained from its research contracts as a result of Defendant's wrongful conduct;
- F. An award of costs of suit and attorneys' fees, as allowable by law;
- G. An award of pre-judgment and post-judgment interest, as provided by law;
- H. Leave to amend this Complaint to conform to the evidence produced at trial; and
- I. Such other and further relief as this Court may deem just and proper.

X. DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury on all claims so triable.

Respectfully submitted,

Dated: July 5, 2017

TOUSLEY BRAIN STEPHENS PLLC

By: s/ Kim D. Stephens

Kim D. Stephens
kstephens@tousley.com
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
Tel: 206.682.5600
Fax: 206.682.2992

Tina Wolfson*
twolfson@ahdootwolfson.com
AHDoot AND WOLFSON, PC
1016 Palm Avenue
West Hollywood, CA 90069
Tel: 310.474.9111
Fax: 310.474.8585
* *pro hac vice* application forthcoming

0099/002/477705.1